

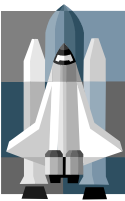
Low Density Parity Check Codes: Bandwidth Efficient Channel Coding

Wai Fong, Shu Lin, Gary Maki and Pen-Shu Yeh

Earth Science Technology Conference
June 24-26, 2003
College Park, MD



Program Objective



- Identify high coding rate (>0.5) Low Density Parity Check Codes (LDPC) for bandwidth efficiency on near-Earth satellites.
- Develop a Flight LDPC encoder application specific integrated circuit (ASIC) for high data rates.
- Subsequently, develop a ground ASIC LDPC decoder.
- In parallel, develop field programmable gate array (FPGA) versions to help evaluate possible architectures and verify performance.



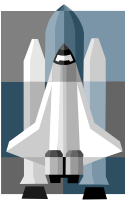
LDPCC Background



- Shannon 1948 proved the Noisy Channel Coding Theorem based on the concept of “random coding.” (The genesis of Coding Theory)
- Elias 1955 showed that randomly chosen parity block codes of long length can perform as well as any code.
- Gallager 1960 invented LDPCC in PhD thesis based on a relatively simple decoder.
- Largely ignored by the coding community until Mackay 1996 showed that LDPCC have near-Shannon limit performance.
- Rediscovery prompted by the invention of Turbo Codes (Berrou1993).
- Large amount of computer generated (CG)-LDPCC based on semi-random construction research since 1996.
- Kou, Lin and Fossorier 2001 presented the first structured LDPCC based on Euclidean Geometry (EG) and demonstrated that random construction is not necessary to produce near-Shannon limit performance. (NASA/GSFC funded research)
- Two EG-LDPCC were proposed for CCSDS standardization. It is these codes that are chosen for Flight ASIC implementation.



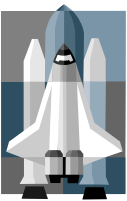
Block Codes Basics



- Consider a binary field $\mathbf{F}_2 =: (\{0, 1\}, +, *)$.
- Then $\mathbf{F}_2^n =: \text{the } n\text{-dimensional vector space over } \mathbf{F}_2 \text{ where the elements are } 2^n \text{ } n\text{-tuples.}$
- **Definition:** An (n, k) linear block code with data word length k and codeword length n is a k -dimensional subspace of \mathbf{F}_2^n .
- The code rate $R =: k/n$
- Minimum distance of a block code $d_{\min} =: \text{minimum weight or least number of ones of all codewords (except the all zero codeword.)}$



Block Code Encoding Process



- In matrix form:

$$\bar{\mathbf{c}} = \bar{\mathbf{u}} \mathbf{G}$$

where,

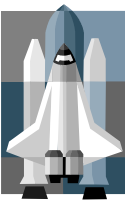
$\bar{\mathbf{u}}$ is the information sequence of length k

$\bar{\mathbf{c}}$ is the codeword of length n

\mathbf{G} is the generator matrix of dim. $k \times n$



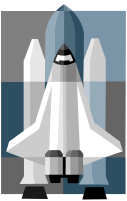
General Hard Decision Block Code Decoding Process



1. Calculate the syndrome (symptom of the corrupted codeword).
2. Identify it's associated error pattern (select the pattern with the smallest number of bit errors).
3. Remove this error pattern from the received word to produce corrected word.



Syndrome Calculation



Syndrome is defined as:

$$\bar{\mathbf{s}} = \bar{\mathbf{r}} \mathbf{H}^T$$

where,

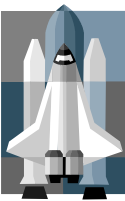
$\bar{\mathbf{r}}$ is the received codeword of length n

$\bar{\mathbf{s}}$ is the syndrome of length $n-k$

\mathbf{H} is the parity-check matrix of dim. $(n-k) \times n$



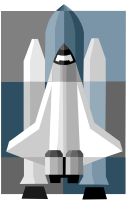
General Soft Decision Decoding Process



- Also called maximum APP (MAP) decoding or maximum likelihood decoding (when all codewords are equally likely).
- Based on samples from the symbol synchronizer.
- Calculate the Euclidean distance between received symbol with every expected codeword.
- Determine the most probable or the nearest codeword.
- Output that codeword.
- Complexity on the order of 2^k real number calculations.
- Not practical except for very small k block codes.
- Provides greater than 2 dB performance improvement over hard decision decoding.



Large Block Codes Decoding Problem



- How to practically accomplish maximum likelihood or MAP decoding with large block sizes?
- Gallager's answer: LDPC can achieve near-MAP decoding performance by inventing an iterative decoder whose complexity is proportional to the total number of 1's in the \mathbf{H} matrix.



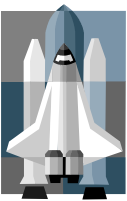
LDPCC Definition



- A regular LDPCC is a linear block code whose parity check matrix H contains a constant number of 1's per column and a constant number of 1's per row.
- An irregular LDPCC has an H matrix with a variable number of 1's per column or row.
- Generally large block codes with the ratio of the total number of ones to the total number of bits in the H matrix to be a very small number ($\ll 0.5$)
- Most LDPC codes are regular and irregular CG-LDPCC.
- CG-LDPCC requires on the order of n^2 operations for encoding.
- EG-LDPCC are structured regular codes which are cyclic or quasi-cyclic in construction.
- EG-LDPCC require on the order of n operations to encode.



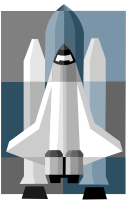
Comparison to Turbo Codes



- Similarities
 - Both codes are decoder centric coding techniques
 - Both codes exhibit BER performance are near-channel capacity
 - Both codes have decoders that use a posteriori probability (APP) metrics.
 - Both codes use a form of Belief Propagation/Message Passing based decoding.
- Differences
 - LDPC are not concatenated codes
 - LDPC do not require an interleaver
 - LDPC do not use multiple Viterbi decoders
 - LDPC are inherently parallel and thus are faster to decode
 - Some LDPC have very low error floors



Relating G and H Matrices



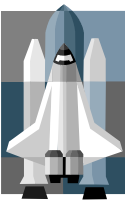
- It can be shown that:

$$\mathbf{GH}^T = \bar{\mathbf{0}}$$

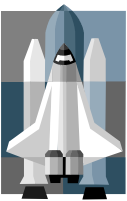
- Once G is defined then an H can be derived.
- The opposite case is also true.
- This is does not produce a unique solution.



EG-LDPCC Advantages Over CG-LDPCC



- Cyclic EG codes can be decoded with various algorithms, from hard-decision (majority logic) to soft-decision (message passing) and weighted hard-decision.
- EG-LDPCC have larger d_{\min} and therefore lower error floors $< 10^{-10}$ BER
- Larger d_{\min} also means better frame error rate (FER) performance.
- EG-LDPCC provide easy encoder design and lower complexity.
 - Place and routing is simpler.
 - Encoding consists of a chain of flip flops.
 - Design of decoder is faster since computational elements are the same.
 - Decoding iterations can be phased or pipelined allowing for a smaller ASIC or FPGA.
- Lower encoder complexity means less demand on spacecraft power system which benefits size and weight.
- In general, EG codes require less iterations and can decode faster than CG codes.



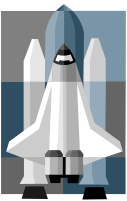
EG-LDPCC H matrix

1	0	0	1	0	0	0	1	0	0	0	1	1	0	0
0	0	1	0	1	0	1	0	0	1	0	0	0	1	0
1	1	0	0	0	0	0	1	0	1	0	0	1	0	0
0	0	0	1	0	1	0	0	0	0	0	0	0	0	1
0	0	1	0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	0	1	0	0	0	1	0	0	1	0	0	0
0	0	0	0	0	1	1	0	0	0	0	0	0	1	1
0	1	0	0	0	0	1	0	0	1	0	0	0	0	0
0	0	1	0	1	0	0	0	1	0	0	0	0	0	0
0	1	0	1	0	1	0	0	0	0	1	0	1	0	1

0	0	0	0	0	1	1	0	1	0	0	0	0	0	1
1	0	0	0	0	0	1	1	0	1	0	0	0	0	0
0	1	0	0	0	0	0	1	1	0	1	0	0	0	0
0	0	1	0	0	0	0	0	1	1	0	1	0	0	0
0	0	0	1	0	0	0	0	0	1	1	0	1	0	0
0	0	0	0	1	0	0	0	0	0	1	1	0	1	0
0	0	0	0	0	1	0	0	0	0	0	1	1	0	1
1	0	0	0	0	0	1	0	0	0	0	0	1	1	0
0	1	0	0	0	0	0	1	0	0	0	0	0	1	1
1	0	1	0	0	0	0	0	1	0	0	0	0	0	1
1	1	0	1	0	0	0	0	0	1	0	0	0	0	0
0	1	1	0	1	0	0	0	0	0	1	0	0	0	0
0	0	1	1	0	1	0	0	0	0	0	1	0	0	0
0	0	0	1	1	0	1	0	0	0	0	0	1	0	0
0	0	0	0	1	1	0	1	0	0	0	0	0	1	0



LDPCC Decoder



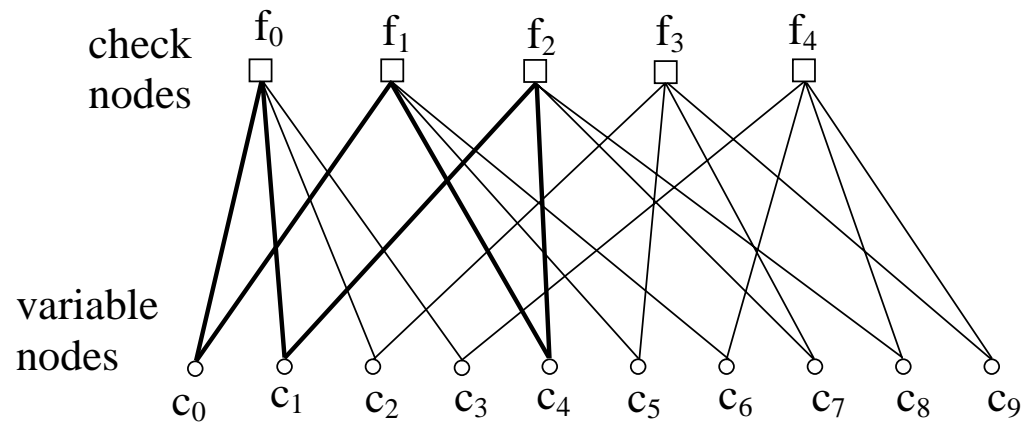
- Decoder can be represented as a message passing algorithm based on a bipartite (Tanner) graph made up of check nodes and variable nodes.
- Number of check nodes is $n-k$ and number of variable nodes is n .
- Connections or edges between check and variable nodes are defined by a 1 in the parity-check matrix \mathbf{H} .
- Messages which are extrinsic information based on APP are passed along edges.
- A full iteration is defined as a cycle of message passing from the variable nodes to check nodes and back.
- The decoder is initialized by soft-decision information received codeword.
- Each full iteration is completed by a hard-decision syndrome calculation.
- If a syndrome is detected, another iteration begins.
- If no syndrome is detected, a valid codeword is found and the decoder stops.



LDPCC Tanner Graph



$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$





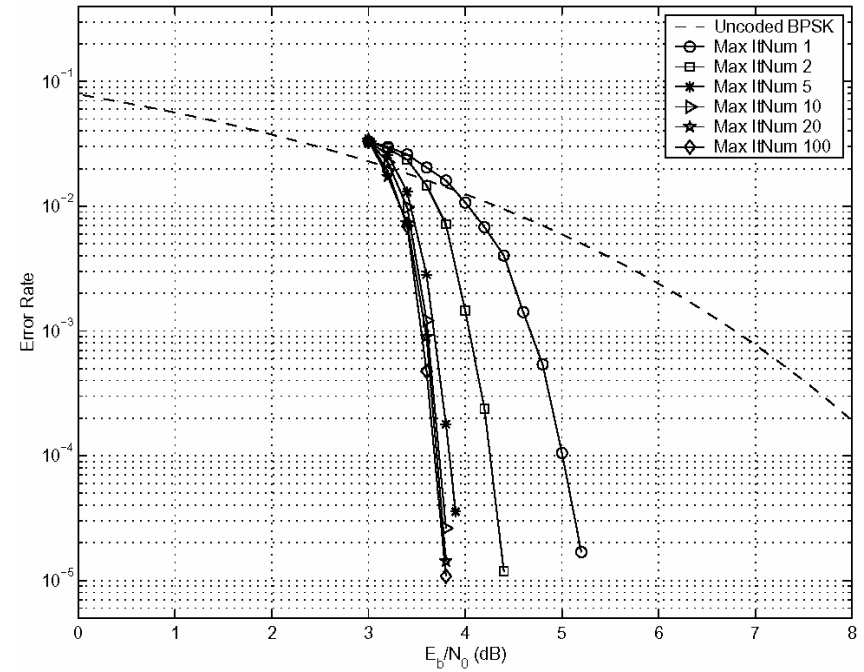
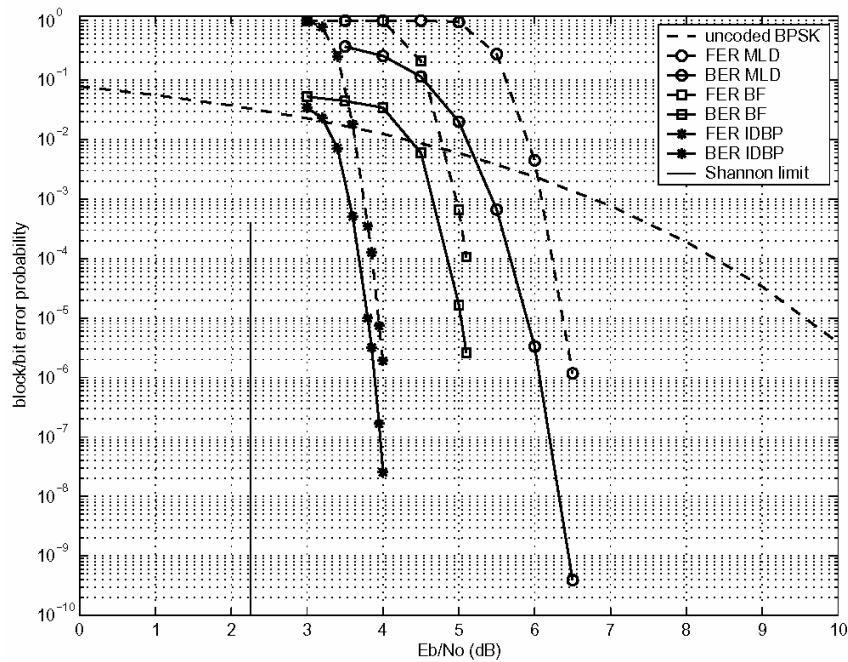
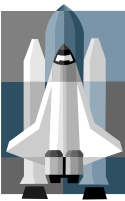
Selected EG-LDPCC



- Two codes: EG-LDPCC (4095, 3367) (or shorten to (4088, 3360)) $R = 0.822$ and EG-LDPCC (8176, 7156) $R = 0.875$.
- $d_{\min} = 65$ for EG-LDPCC (4095, 3367) and $d_{\min} > 7$ for EG-LDPCC (8176, 7156).
- Both codes have been simulated to $> 10^{-10}$ BER with no error floor.
- EG-LDPCC (4095, 3367) is a cyclic code and EG-LDPCC (8176, 7156) is a quasi-cyclic code.
- Both codes can be encoded with a sequence of shift registers.
- Both codes have very fast iterative convergence.

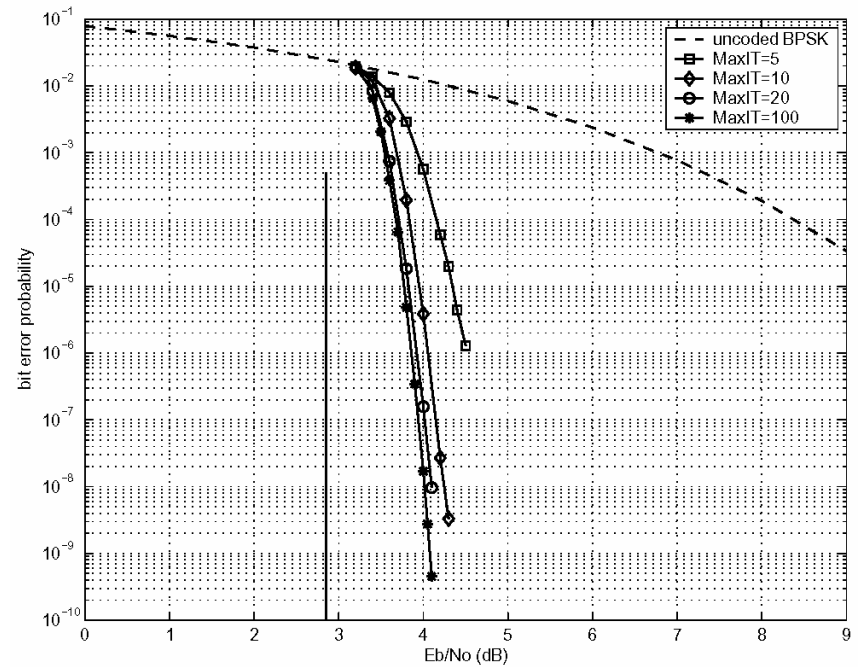
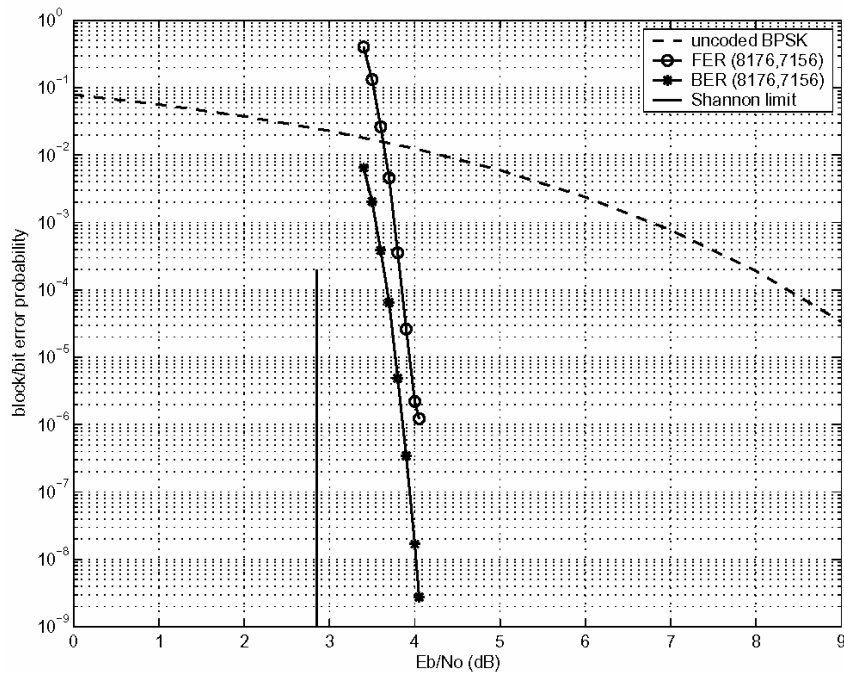


EG-LDPCC (4095, 3367) Performance



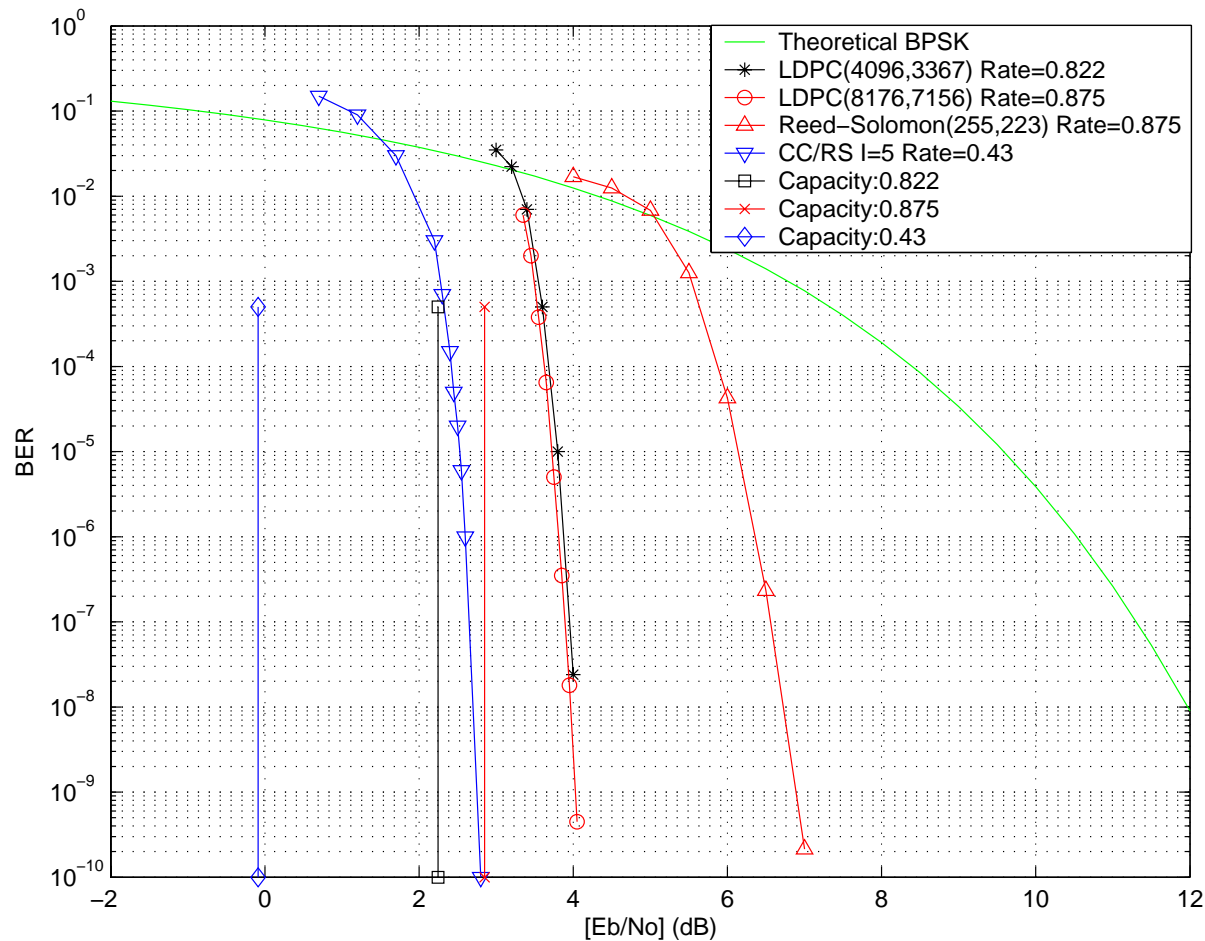
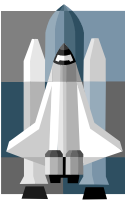


EG-LDPCC (8176, 7156) Performance



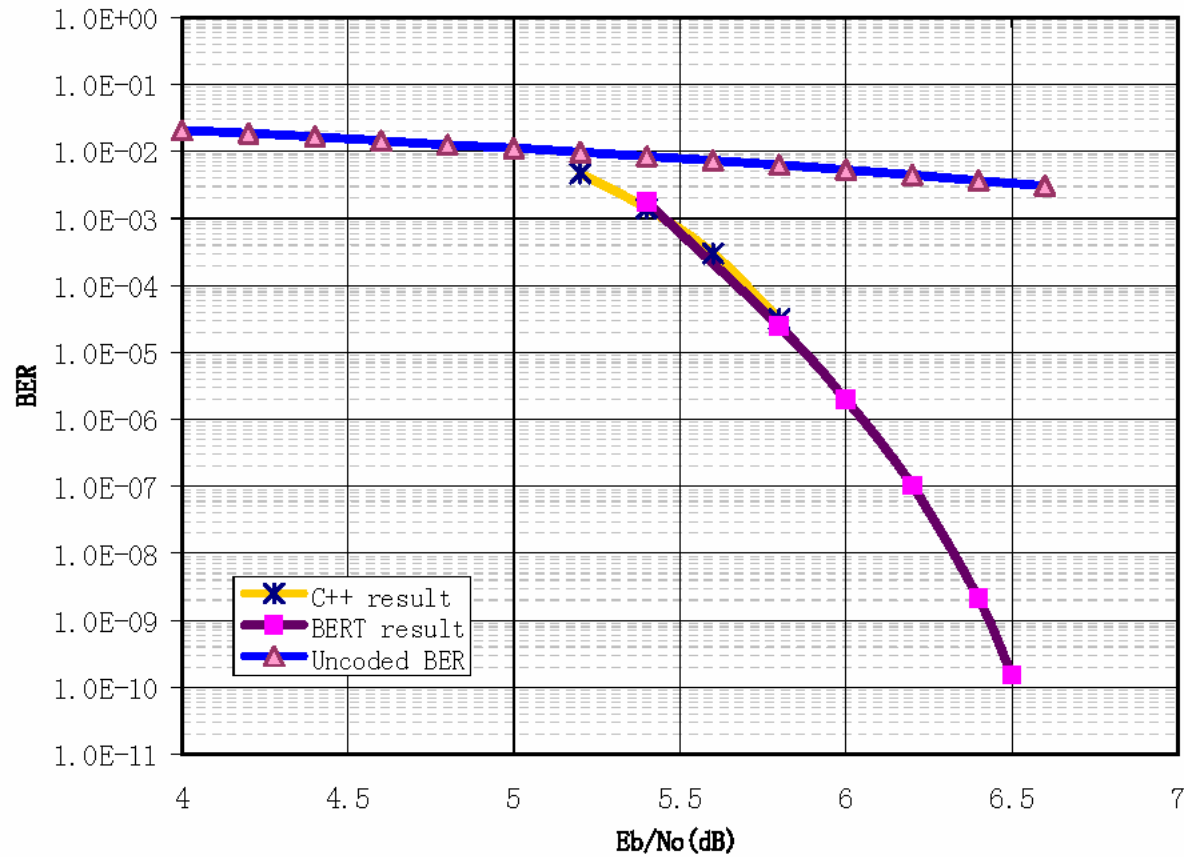


EG-LDPCC Versus Standard Codes



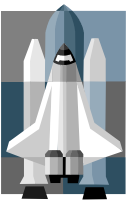


EG-LDPCC (4095, 3367) Measured Performance





Status



- There are two parallel development tracks: 1. Flight ASIC encoder along with the ASIC decoder and 2. the FPGA encoders and decoders.
- Currently, EG-LDPCC (4095, 3367) has been designed for the flight ASIC and has been simulated to > 1 Gbps operation.
- The encoder for EG-LDPCC (8176, 7156) is currently being developed.
- Flight ASIC encoder fabrication containing both codes is scheduled to be completed by the first quarter of 2004.
- The EG-LDPCC (4095, 3367) FPGA encoder as well as its FPGA Majority Logic decoder has been tested at 400 Mbps.
- Currently, an EG-LDPCC (4095, 3367) FPGA Belief Propagation decoder has been designed and is being optimized for operating speed. Its testing will be completed by the end of August 2003.
- An FPGA encoder and decoder of EG-LDPCC (8176, 7156) will probably be completed by end of 2003.
- The Belief Propagation ASIC decoders for EG-LDPCC (4095, 3367) and EG-LDPCC (8176, 7156) are undergoing an architectural study.
- Fabrication won't be completed until first quarter 2005.